A Four Entities Mutual Authentication Technique for Vehicular Ad Hoc Network

Pijush Kanti Bhattacharjee, Member, IACSIT

Abstract—Hacking and threats are increasing with the enhanced population of wireless traffic. Authentication of correct mobile nodes in Vehicular Ad Hoc Network is an extremely challenging issue to the researchers. Vehicular Ad Hoc Network (VANET) is one of the wireless ad hoc networks which are based on IEEE 802.11 wireless standard enabling vehicle to vehicle and roadside communications through air interface. Information (voice, message, data, image etc) are routed in the cells or networks, any node or person can hack or tamper the information. In this paper, a mutual authentication technique is proposed which verifies the authenticity of the calling and the called subscribers (nodes or vehicle drivers) as well as the calling node with the network by calling subscriber’s password, SIM and biometric properties of the calling subscriber. Two biometric parameters are used in which one biometric parameter is stored in his own node and the other biometric parameter taken as frequency of Flipping or Clapping sound of each subscriber, called certified document (CD), is stored at the other nodes or the server (PDSN or MSC). An algorithm is developed by these four entities to check this authentication process, named four entities mutual authentication technique for Vehicular Ad Hoc Network (VANET).

Index Terms—Biometric property, Certified Document, Clapping sound, CSMA/CA, DSRC, Distributed Coordination Function, Flipping sound, MAC layer, Mutual Authentication, Packet Switching, Password, Vehicular Ad Hoc Network.

I. INTRODUCTION

Vehicular Ad Hoc Network [5]-[8] is an emerging field in the ad hoc network keeping in view of vehicle to vehicle direct communications and also connecting to the basic mobile network [1]-[4] with Internet. Thus it provides coverage all regions in the world, especially in remote and less dense populated area where the normal mobile communications are not economically viable like long distance roadways or railway trucks etc. In this case ad hoc network is the best solution. Two types of ad hoc wireless networks are invented, one is Mobile Ad Hoc Network (MANET) and the other is Vehicular Ad Hoc Network (VANET) [5]-[8]. MANET and VANET are self forming network i.e. they can work without any centralized control like Base Station (BTS) or Switch (BSC, MSC etc) in mobile network or Access Point (AP) in LAN.

Each terminal or node (either mobile phone or computer) in a MANET or a VANET acts both as a data or voice terminal and router or switch [5]-[8]. A node in a cell communicates with the other nodes in its transmitting range through wireless medium. A VANET is a subset of a MANET. In a VANET, certain number of moving vehicles in a small region constitutes a cell. It means that the range of wireless signal i.e. transmitting zone from a moving vehicle is within a limited area. A vehicle, called a node, can do transmitting, receiving and routing (connecting) to other nodes without any help of any switch like base station (BTS) in mobile network or Access Point (AP) in LAN. Also the moving vehicle in a VANET cell can be connected to other nodes in other cell or other network with the help of basic mobile network, Internet etc. Thus total connectivity in a VANET is assured. VANET are also known under different name like DSRC (Dedicated Short Range Communications), Inter Vehicle Communications (IVC) etc. Thus VANET will help the drivers of vehicles to communicate the information in form of voice, data, image etc and ensure safe journey by minimizing road accidents, diverting or instructing the vehicle’s direction in less populated roads avoiding traffic jam etc. Vehicles in a VANET are having high degree of mobility i.e. the vehicles are moving very fast, especially in high ways. As a result the two vehicles are in a direct communication range staying about one minute time only i.e. two vehicles remain in one cell about 1 minute time when they are moving parallel direction or even less than 1 minute when they are in opposite direction. Due to this, VANET cell configuration and number of nodes in a particular cell is always changing in nature.

VANET is based on IEEE 802.11 wireless standard [6]-[8] which is mainly framed for WLAN, WiFi, MANET and VANET.

Initially 802.11 are implemented on WLAN at a speed of 1 or 2 Mbps (very slow) in 1997. Then IEEE 802.11 protocol family is upgraded to different versions. 802.11a uses OFDM (Orthogonal Frequency Division Multiplexing) modulation to deliver upto 54 Mbps in the wider frequency 5 GHz ISM band. 802.11b applies HR-DSSS (High Rate Direct Sequence Spread Spectrum) to achieve 11 Mbps in 2.4 GHz ISM band. 802.11g implements OFDM modulation, but operates narrow 2.4 GHz ISM band. The FCC (Federal Communications Commission) suggests for VANET frequency spectrum (bandwidth) of 75 MHz in the range of 5.850 GHz to 5.925 GHz in USA. In this seven channels are fragmented, having each 10 MHz bandwidth. Six channels are used for services and one channel is used for control purpose like broadcast services e.g. safety message, announcement etc. The 802.11 protocols apply CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) with acknowledgements for reliable communications and avoiding collision between packets. In a VANET, MAC (Medium Access Control) layer
determines a contention based access protocol, termed DCF (Distributed Coordination Function). Actually MAC sublayer determines how the channel is allocated i.e. who will transmit next. Above MAC, there is LLC (Logic Line Control) to hide the difference between different 802 variants.

A vehicle (node) can make wireless call to any other vehicles moving in its own cell or in the other cells or to other network like basic mobile services including Internet as shown in Fig. 1. If transmitting power of a node (vehicle) increases in a VANET, signal from the node will spread more area i.e. the cell size becomes large, but throughput of the network i.e. information handling capacity will decrease. Again the number of hops (cells) increases in a region, expected path of life decreases. The transmission signal in a VANET is interference due to multipath fading, different type of noise, power supply fluctuation and out of cover range (mobility) etc. All vehicles (nodes) in a cell can be assigned station code or ID like Internet Protocol (IP) address and the packets (data) are routed to the node ID address. This station code is liable to change very frequently as the vehicles are going inside or leaving outside a cell in a rapid manner, so in a node ID address, cell number or cell ID is also mentioned e.g. a node having ID 2C32 means, it moves in the Cell ID 2C having node number 32. Since information (voice, message, data, image etc) are routed in the cell (network), any node within or beyond the cell can monitor or tamper the information. To avoid hacking or corrupting information, certain authentication (security) [9] schemes in the VANET communications are to be taken.

Now four entities mutual authentication technique is proposed for identifying correct nodes (subscribers) as well as a node or a basic mobile network or other networks.

Four Entities (4-E) mutual authentication technique is a technique to authenticate for communicating subscriber according to what you know (Password), what you have (SIM), what you are (Biometric entity) and what you posses (Certified Document). This mutual authenticity is verified by applying identifier, password, biometric entities of the subscriber, one biometric parameter stored in its node and the other biometric parameter stored in the other nodes and the server and the switch as certified document (CD). Here I am taking frequency of flipping sound of a subscriber as certified document (CD), since flipping sound is more convenient to produce than clapping sound at the time of connecting a mobile call. Flipping and Clapping sound depends on physical structure, heart and muscle capacity and other body parameters of a subscriber and its frequency remains almost constant for a subscriber (vehicle driver).

II. PROPOSED FOUR ENTITIES MUTUAL AUTHENTICATION TECHNIQUE FOR VANET

The proposed four entities (4-E) authentication technique is a collection of four different phases, namely, Subscriber (node) Enrollment Phase, Calling Subscriber (node) Authentication Phase, Called Subscriber or Network Authentication Phase and Subscriber Password Change Phase.

A. Subscriber Enrollment Phase

In subscriber enrollment phase, a subscriber is enrolled to all other nodes or particular network AAA server or switch (MSC). This phase is executed only once for one subscriber.

SE1: The subscriber chooses his identifier I, password P

and Biometric property B i.e. the extracted template of biometric entity of the subscriber (Vehicle driver). Now a subscriber can make clapping sound by striking the two hand palms simultaneously and flipping sound by rubbing top most portions of the thumb and the middle finger. Since clapping sound is difficult to use at the starting time of a mobile call, therefore flipping sound is more convenient. F is average value of flipping frequency of a subscriber (vehicle driver) from five consecutive flipping sounds which are measured by sophisticated electronics instrument in Hz. Thereafter the subscriber passes these information (I, P, B) secretly to the authority concerned (VANET service provider) for initialization the node and F for storing in the all other nodes or the server or the switch.

SE2: The other nodes or AAA server or switch has received the enrollment request from the subscriber with I, P, B, F data and executes the following tasks.

SE2.1: Stores F into all the nodes and the AAA server and the switch.

SE2.2: Computes G = h(\text{B} \oplus \text{F}), h(.) is a one-way hash function and \text{B} is a bitwise XOR operation.

SE2.3: Stores the parameters \{B, G, I, K, P\} into the particular node (subscriber) asking for enrollment.

B. Calling Subscriber (node) Authentication Phase

This phase is executed every time when a subscriber (node or vehicle) is attempting to make a call connection.

The calling subscriber (vehicle driver) enters his identifier I, password P’ and imprints his biometric entity B’ from the biometric device in the node e.g. caller’s fingerprint, voiceprint, clapping sound, flipping sound, face image etc are taken by its associated electronics circuit installed in the node, ultimately these template’s array or matrix information represents biometric entity B’. The calling subscriber makes flipping sound. The frequency of flipping sound (F’) is computed by highly sophisticated electronics device in the node which can analyze exact frequency range in Hz say 2534 Hz.

SA1: Calling node requests for F from the called node or
the AAA server or the switch.

SA2: The called subscriber or AAA server or switch sends F to the calling subscriber through paging or secured channel.

SA3: The calling node (subscriber) checks that $|F \sim F'|$ is tolerable (within certain range) or not. If it is tolerable then the calling node performs the following tasks, otherwise terminates the communication.

SA3.1: The MS computes $L = h(F \oplus F')$, Then checks whether $L$ is equal to the $h(F)$ or not. If $L = h(F)$ when $G = h(P' \oplus B')$, then checks whether $L$ is equal to the $h(F)$ or not. Otherwise, the calling subscriber checks that $|F \sim F'|$ is tolerable (within certain range) or not. If it is tolerable, the subscriber performs the next tasks, otherwise terminates the communication.

SA3.2: Computes $O = (G \oplus h(T))$, where $T$ is the current time while the calling subscriber initializing the call.

SA3.3: Computes $N = h(\oplus \oplus h(T))$.

SA3.4: Sends the communication request $\{O, N, T\}$ to the called node or the AAA server or the switch.

SA4: The called node or the AAA server or the switch has received the communication request $\{O, N, T\}$ at time $T*$ and executes the followings tasks.

SA4.1: Checks the difference between $T*$ and $T$ i.e. whether $[T* \sim T]$ is valid time interval for measuring transmission delay or not. If it is correct (valid) then the called node or the AAA server or the switch performs the next tasks, otherwise terminates communication.

SA4.2: Computes $N' = h(\oplus \oplus O)$.

SA4.3: The called node or the AAA server or the switch checks whether $N \neq N'$. If it holds good, the called node or the AAA server or the switch accepts the communication request of the calling subscriber.

If $N \neq N'$, the called node or the AAA server or the switch cancels the communication request of the calling node (subscriber) due to failure of calling subscriber (Calling node) authentication phase.

C. Called Subscriber or Network Authentication Phase

The called subscriber (node) or the network (switch or server) is verified in this phase, this is executed when the calling subscriber is authentic.

NA1: Called node or AAA server or switch requests for I, P, B from calling node.

NA2: Calling node sends I, P, B to the called node or the AAA server or the switch through secured channel.

NA3: Called node or AAA server or switch computes that $M = h(T** \oplus \oplus h(F \oplus \oplus h(I \oplus P \oplus B)))$, where $T**$ is current time.

NA4: Called node or AAA server or switch sends $M, T**$ to the calling subscriber through a paging or secured channel.

Suppose calling subscriber receives $M, T**$ at time $T***$.

NA5: Calling node checks the difference between $T***$ and $T**$ i.e. whether $[T*** \sim T**]$ is valid time interval for transmission delay or not. If it is correct, then the calling node performs the next tasks.

NA5.1: Calling node computes, $M' = h(T** \oplus \oplus \oplus K))$

NA5.2: The calling node checks whether $M = M'$. If it holds, then the calling subscriber is connected either to the desired called node or the network (AAA server or switch).

If $M \neq M'$, call request is terminated, hence calling subscriber or network authentication fails.

D. Subscriber Password Change Phase

This phase is executed when any subscriber (node) wants to change his password $P$ by the new password $P^*$. The subscriber selects a new password $P^*$, enters it. If it is correct (valid), the subscriber performs the next task, otherwise terminates password change request.

SP1: Subscriber requests for $F$ from other nodes or AAA server or switch.

SP2: The other nodes or AAA server or switch sends $F$ to the subscriber through paging or secured channel.

SP3: The subscriber checks that $|F \sim F'|$ is tolerable (within certain range) or not. If it is tolerable (valid), the subscriber performs the next task, otherwise terminates password change request.

SP4: The subscriber verifies the entered $I$ and $P^*$ with the stored values of $I$ and $P$ in the node and the biometric entity of the subscriber $B'$ with the stored values $B$. If all the verifications are matched correctly, then the subscriber executes the following tasks.

SP5: Asks the subscriber to enter a new password and he chooses a new password $P^*$ and enters it.

SP6: Computes $G^* = h(I \oplus P^* \oplus B)$ and $K^* = (h(G \oplus G^*))$.

SP7: The $P^*$, $G^*$ and $K^*$ are stored in the place of $P$, $G$ and $K$ respectively.

III. ADVANTAGES OF THE PROPOSED AUTHENTICATION TECHNIQUE

The proposed authentication system is working in two ways i.e. it makes connections between the authentic or desired subscribers (nodes) or to its home or appropriate network by verifying mutually. By adopting this mutual check up system, huge amount of data, messages, information etc. are exchanged between the nodes (calling and called) or the network (MSC or PDSN) smoothly in a vehicular ad hoc network communications. It has lot of advantages which are specifically listed below:

(a) Subscriber authentication is checked by the physical characteristics of the user i.e. biometric property.

(b) One way hash function and XOR operation are only used which minimizes computation complexity and time.

(c) Many storing document with the same identifier can be allocated for service i.e. the same login (identifier) from different document can not make connection to the network.

(d) Any subscriber’s identifier (I), password (P), biometric property (B) are not required to store in the other nodes or the AAA server or the switch, hence these information can not be hacked from the other nodes or the server or the switch.

(e) The user can freely change his password and change the password as and when necessary.

(f) I, P, B can be reset or changed with user’s request by the authority (VANET service provider) without concerning the other nodes or server or switch, but certified document i.e. biometric entity (B) is only changed by consulting the other nodes or the server or the switch.
IV. EXPERIMENTAL RESULTS FROM THE PROPOSED ALGORITHM

The proposed algorithm is tested by exploring in C-language program under Linux environment. I obtain very fairly result which can be easily implemented in the VANET network for authentication purpose. The experimental results are described below. The following parameters are considered for executing the program. In case of the biometric entity, for simplicity I have taken twenty numbers of alphabetic characters as mentioned below.

Subvertiser (node) or user Identifier (I) is taken “IdentityofSubscriber”.
Subvertiser (node) or user Password (P) is taken “User’sAuthentication”.
Subvertiser (node) or user Biometric Entity (B) is “BiometricFingerprint”.
Subvertiser (node) or user Average Flipping frequency (F) is “2653” Hz.

Timestamps are considered like followings

T - 20-07-2009, 10:10
T* - 20-07-2009, 10:11
T** - 20-07-2009, 10:12
T*** - 20-07-2009, 10:13

Timestamps are within valid time intervals.

A. Subvertiser Enrollment Phase

A subscriber (node) chooses his identifier (I), password (P), biometric property (B and F) as mentioned above and submits this information to the all other nodes or the AAA server or the switch. The other nodes or the AAA server or the switch computes G, K and supplies to the subscriber for storing and stores F in the other nodes and the AAA server and the switch. This is done only first time for enrolling a subscriber in a VANET. Results are shown below:

Subvertiser Password (P) = 55736572277341757468656e746963617469666e
G = h(I P B) = 1a5faeec6b6e3a17d38d03421a42c3135f7118c5
K = h(K B G) = 954b44b8e6429c814da20e5851bd25e0f5099fe

B. Calling Subvertiser (node) Authentication Phase

At the starting time of communication, firstly the calling subscriber (node) checks or matches the subscriber identifier (I), password (P), biometric property (B and F) and flipping frequency (F) by verifying whether L = h(F). Then Calling node computes O and N and sends to the called node or the AAA server or the switch. Results of Calling Subscriber Authentication Phase are mentioned below:

O = G h(T) = 5e8170474c8a6cfe1fcb7c32dd18432317e870a8a
N = h(K h(T)) = 9774438c408dc411db9f90aca7b8456e5b2064772

After receiving those, the called node or the AAA server or the switch computes N′ and compares it with N.

N′ = h(F O) = 9774438c408dc411db9f90aca7b8456e5b2064772
As N = N′, the called subscriber (node) or the AAA server or the switch certifies that the calling subscriber is authentic. So the called subscriber or the server or switch accepts the communication request of the calling subscriber.

C. Called Subvertiser or Network Authentication Phase

The called subscriber’s (node) or network’s genuineness is ascertained by the following steps. First the called subscriber or the AAA server or the switch computes M by ascertaining I, P, B from calling node. Thereafter the called node or the AAA server or the switch sends M to the calling node. After receiving M, the calling node (subscriber) computes M′ and compares it with M. Results of Network Authentication Phase is described below:

M = h(T* h(T h(F) h(I P B))) = b113399a400d12cb73a7efa7e590e0146edd94ac
M′ = h(T* h(T K)) = b113399a400d12cb73a7efa7e590e0146edd94ac
As M = M′, the calling node certifies that the called node is authentic.

V. CONCLUSION

In this paper, the proposed four entities mutual authentication technique between the nodes (vehicles) or the node and the network is described. By applying this technique, the Vehicular Ad Hoc network communications are completely restricted within the proper authentic subscribers (vehicles) and also the network. This technique is very fast operating since my proposed algorithm tested under C-language programming. Therefore, this authentication method can be applied in real time basis for all sort of Vehicular Ad Hoc Network.

REFERENCES

Dr. Pijush Kanti Bhattacharjee is associated with the study of Engineering, Management, Law, Indo-Allopathy, Herbal, Homeopathic and Yogic medicines. He is having qualifications ME, MBA, MDCTech, AMIE, BSc, BA, LLB, BIASM, CMS, PET, EDT, FWT, DATHRY, BMus, KOVID, DH, ACE, FDCI etc. He worked in Department of Telecommunications (DoT), Govt. of India as an Engineer from June 1981 to Jan 2007 (26 years), lastly holding Assistant Director post at RTEC [ER], DoT, Kolkata, India. Thereafter, he worked at IMPS College of Engineering and Technology, Malda, WB, India as an Assistant Professor in Electronics and Communication Engineering Department from Jan, 2007 to Feb, 2008 and Feb, 2008 to Dec, 2008 at Haldia Institute of Technology, Haldia, WB, India. In Dec, 2008 he joined at Bengal Institute of Technology and Management, Santiniketan, WB, India in the same post and department. He has written two books “Telecommunications India” & “Computer”. He is a Member of IE, ISTE, IAPQR, IIM, ARP, India; CSTA, USA; IACSIT, Singapore and IAENG, Hongkong. His research interests are in Telecommunications including Mobile Communications, Network Security, VLSI, Nanotechnology etc.